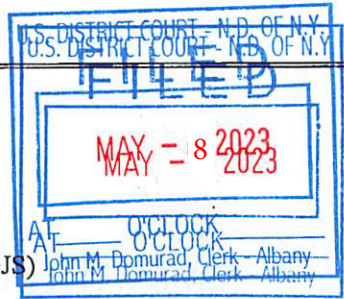


Case No. 1:23-mj- 268 (DJS)



I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Northern District of New York, there is now concealed (*identify the person or describe the property to be seized*):
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 922(g)(1)

21 U.S.C. § 841(a)(1)

Offense Description

Felon in Possession

Possession with Intent to Distribute

The application is based on these facts:

See attached affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Herbert D. Hall, DEA TFO

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone (specify reliable electronic means).

Date: May 8, 2023

City and state: Albany, NY

m. P. 4.1 by Telephone (specify reliable electronic means).



Judge's signature

Hon. Daniel J. Stewart, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR NORTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE APPLICATION
FOR A SEARCH WARRANT OF ONE
BLUE APPLE IPHONE, ONE BLACK TCL
CELLPHONE, AND ONE BLACK APPLE
IPHONE

Case No. 1:23-MJ- (DJS)

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41
FOR A WARRANT TO SEARCH AND SEIZE

I, Drug Enforcement Administration Task Force Officer Herbert D. Hall, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search: one blue Apple iPhone, one black TCL cellphone, and one black Apple iPhone (hereinafter collectively referred to as the "SUBJECT DEVICES"), currently located in law enforcement possession, as described in Attachment A, and the extraction from the SUBJECT DEVICES of electronically stored information described in Attachment B.

2. I am an "investigative or law enforcement officer of the United States" within the meaning of Section 2510 (7) of Title 18, United States Code, that is, an officer of the United States who is empowered by law to conduct investigations and to make arrests for offenses enumerated in Section 2516, Title 18, United States Code. I am currently employed as an Investigator with the Saratoga County (NY) Sheriff's Office ("SCSO"), located in Ballston Spa, New York. I am assigned to the SCSO Narcotics Unit. Furthermore, I am assigned to the Drug Enforcement Administration ("DEA") Capital District Drug Enforcement Task Force ("CDDETF") located in Latham, New York. I have been employed by the SCSO since July of

1998 and was promoted to Investigator in December of 2005. In January of 2012, I was assigned to the SCSO Narcotics Unit and assigned to the DEA CDDETF in September of 2015.

3. During my career in law enforcement, I have taken part in hundreds of narcotics and gang-related investigations and numerous narcotics, gang and conspiracy-related training classes instructed by local, state and federal agencies. I have arrested hundreds of individuals for violations of federal and state narcotics laws. I have participated in the execution of in excess of one hundred search warrants resulting in the seizure of narcotics and proceeds thereof. I have also attended several schools and seminars, including those given by the DEA, New York/New Jersey High Intensity Drug Trafficking Area program ("HIDTA") and other agencies of which concern the enforcement of the laws prohibiting the trafficking of narcotics, guns and money laundering, as well as the packaging and concealment of narcotics. Because of these experiences, I am familiar with the coded language, conduct, and customs of people engaged in conspiracies to violate the drug, gun, and money laundering laws of New York and the United States.

4. I am familiar with the ways in which drug traffickers conduct their business, including, but not limited to, their methods of importing and distributing controlled substances, their use of telephones, instant messaging applications, and social media. I am familiar with drug traffickers using numerical codes, code words, secretive messages, and photos to conduct their transactions. I have conducted and participated in investigation focused on the trafficking and distribution of, but not limited to, marijuana, cocaine, crack cocaine (cocaine base), methamphetamine, heroin, fentanyl, and diverted prescription pills.

5. I make this affidavit from personal knowledge based on my participation in this investigation, including review of reports by myself and/or other law enforcement agents,

communication with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. The information outlined below is provided for the limited purpose of establishing probable cause for a warrant, and does not contain all details or all facts known to me regarding this investigation.

6. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 922(g)(1) (Felon in Possession) and Title 21, United States Code, Section 841(a)(1) (Possession with Intent to Distribute a Controlled Substance) ("TARGET OFFENSES"), have been committed by LESHAWN THOMAS ("THOMAS") and other individual(s) engaged in the commission of these and related crimes, and there is probable cause to search the SUBJECT DEVICES as described below and in Attachment A for fruits, evidence, and instrumentalities of these crimes, as specifically described in Attachment B.

PROBABLE CAUSE FOR THE SUBJECT DEVICES

7. Based upon my training and experience, I know drug traffickers must maintain telephone and address listings of clients and suppliers and keep them immediately available in order to efficiently conduct their drug trafficking business. For example, many drug traffickers maintain cellular telephones that they use to coordinate their drug trafficking; specifically, they use the cellular telephones to communicate with: (1) suppliers about obtaining additional quantities of drugs and negotiate price and logistics related to acquiring those drugs; (2) customers about available inventory, prices, and logistics related to selling the drugs; and (3) co-conspirators about acquiring, storing, and transporting drugs and proceeds generated from the sale of illegal drugs. Based on my training and experience, I also know that those involved in

drug trafficking often use multiple cellular telephones and other electronic devices to facilitate their illegal activities, including access bank accounts, conduct financial transactions, and communicate with co-conspirators about their criminal activities.

8. In or about March 2009, THOMAS was convicted under New York Penal Law §§ 265.03(3) (Criminal Possession of a Weapon in the Second Degree-Loaded Firearm) and 160.15(4) (Robbery in the First Degree – Displays What Appears to be a Firearm). THOMAS was sentenced to fifteen (15) years in prison, to be followed by five years of post-release supervision. Thomas was received by parole on or about November 24, 2021 with a maximum supervision date of on or about November 16, 2023. One of THOMAS’S conditions of release was that he would permit his Parole Officer to visit him at his residence and permit the search and inspection of his person, residence, and property.

9. On or about April 28, 2023, at approximately 9:00 a.m., New York State Parole Officers (“Parole Officers” or “Parole Officer”) conducted a search of THOMAS’S parole-approved residence, which is located at 9714 Maple Pl., Clayville, New York (“residence”), in the Northern District of New York. THOMAS was present, along with his wife and infant child. Upon searching THOMAS’S bedroom, Parole Officers recovered keys to the following vehicles, which were parked outside the residence: a red Mazda (“Mazda”) and a black Honda Accord (“Honda”). The Mazda was a rental car from Enterprise Rent-A-Car and was rented in THOMAS’S name. The Honda is registered to THOMAS. The Officers also discovered four cellular phones in THOMAS’S bedroom, including the SUBJECT DEVICES. The SUBJECT DEVICES were seized and are currently in law enforcement custody at 10 Hastings Drive, Latham, NY.

10. Upon searching the Mazda, two loaded handguns were recovered from the console. When searching the Honda, a bookbag was found in the trunk. Upon unzipping the bookbag, the following items were discovered: five clear plastic bags containing a white-in-color rock and powder substance consistent with cocaine; seven bundles of various money denominations rubber-banded together; and three vacuum-sealed packages, two of which were inside a shopping bag. A TruNarc Scan indicated that the white-in-color rock and powder substance tested positive for cocaine base, with an approximate weight of 292 grams. A TruNarc Scan indicated that the three vacuum-sealed packages tested positive for cocaine, with an approximate aggregate weight of 3.4 kilograms. Based on my training and experience, I know this quantity of cocaine is indicative of drug trafficking and not for personal use.

11. On May 4, 2023, based on the conduct described above, THOMAS was charged by criminal complaint in the Northern District of New York with 21 U.S.C. § 841(a)(1) & (b)(1)(B) (Possession with Intent to Distribute). *See United States v. LeShawn Thomas*, Case No. 5:23-mj-259 (DJS) at Dkt. 1 (Complaint).

12. Accordingly, there is probable cause to believe that evidence of the TARGET OFFENSES will be found on the SUBJECT DEVICES.

TECHNICAL TERMS

13. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or

traditional “land line” telephones. A wireless telephone usually contains a call log, which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic address books; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

14. Based on my training, experience, and research, examining data stored on cellular telephones can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC DEVICES, STORAGE, AND FORENSIC ANALYSIS

15. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

16. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information on the SUBJECT DEVICES that might serve as direct evidence of the TARGET OFFENSES described on the warrant, but also forensic evidence that establishes how a device was used, the purpose of its use, who used it, and

when. There is probable cause to believe that this forensic electronic evidence might be on electronic devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

17. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the SUBJECT DEVICES consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the SUBJECT DEVICES to human inspection in order to determine whether it is evidence described by the warrant.

18. *Manner of execution.* Because this warrant seeks only permission to examine the SUBJECT DEVICES already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

19. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that evidence of criminal offenses, namely, violations of Title 18, United States Code, Section 922(g)(1) (Felon in Possession) and Title 21, United States Code, Section 841(a)(1) (Possession with Intent to Distribute a Controlled Substance), exist and are concealed on the SUBJECT DEVICES, which are currently in law enforcement custody at 10 Hastings Drive, Latham, NY.

Attested to by the affiant,



Herbert D. Hall
Task Force Officer
Drug Enforcement Administration

I, the Hon. Daniel J. Stewart, United States Magistrate Judge, hereby acknowledge that this affidavit was attested by the affiant by telephone on May 8, 2023 in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.



Hon. Daniel J. Stewart
United States Magistrate Judge

ATTACHMENT A

ITEMS TO BE SEARCHED

The items to be search are: one blue Apple iPhone, one black TCL cellphone, and one black Apple iPhone (hereinafter collectively referred to as the “SUBJECT DEVICES”), each of which is currently in law enforcement custody at 10 Hastings Drive, Latham, NY.

This warrant authorizes the forensic examination of the SUBJECT DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

ITEMS TO BE SEIZED AND SEARCHED

All records on the SUBJECT DEVICES described in Attachment A that relate to violations of Title 18, United States Code, Section 922(g)(1) (Felon in Possession) and Title 21, United States Code, Section 841(a)(1) (Possession with Intent to Distribute a Controlled Substance) ("TARGET OFFENSES") committed by LESHAWN THOMAS ("THOMAS") and other individual(s) engaged in the commission of these and related crimes, including:

Computers and Electronic Media

1. The authorization includes the search of electronic data to include deleted data, remnant data and slack space. The seizure and search of computers and electronic media will be conducted in accordance with the affidavit submitted in support of this warrant.
2. Computer hardware, meaning any and all computer equipment, including any electronic storing devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as thumb drives, flash drives, SD (secure digital) cards, fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical and compact storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing, or signaling devices, and electronic tone generating devices); and any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).
3. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems, software, application software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.
4. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

5. Computer passwords and data security devices, meaning any devices, programs, or data, whether themselves in the nature of hardware or software, that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data, or to otherwise render programs or data into usable form.
6. Any computer or electronic records, documents and materials referencing or relating to the above described offenses. Such records, documents or materials, as well as their drafts or modifications, may have been created or stored in various formats, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, video tapes, motion pictures, or photocopies); any mechanical form (such as photographic records, printing or typing); any electrical, electronic or magnetic form (such as tape recordings, cassettes, compact disks); or any information on any electronic or magnetic storage device (such as thumb drives, flash drives, sd (secure digital) cards, floppy diskettes, hard disks, CD-ROMs, DVDs, optical disks, printer buffers, soft cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.
7. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), or any computer or computer system. The form that such information might take includes, but is not limited to, thumb drives, flash drives, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, DVDs, video cassettes, and other media capable of storing magnetic or optical coding.
8. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data used to conduct computer or Internet-based communications, or which contains material or data, obtained through computer or Internet-based communications, including data in the form of electronic records, documents and materials, including those used to facilitate interstate communications, included but not limited to telephone (including mobile telephone) and Internet Service Providers. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding, on computer media, or on media capable of being read by a computer or computer-related equipment, such as thumb drives, flash drives, SD (secure digital) cards, fixed disks, external hard disks, removable hard disk cartridges, CDs, DVDs, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, or other memory storage devices.

Documents, Records and Evidence

9. Records of personal and business activities relating to the operation and ownership of the SUBJECT DEVICES.
10. Any records or documents pertaining to accounts held with Internet Service Providers or of Internet use.
11. Records of address or identifying information for the target(s) of the investigation and any personal or business contacts or associates of his, (however and wherever written, stored or maintained), including contact lists, buddy lists, email lists, ICQ addresses, IRC names (a.k.a., "Nics"), user ID's, eID's (electronic ID numbers) and passwords.
13. Documents and records regarding the ownership and/or possession of the SUBJECT DEVICES.
15. Evidence of software that would allow others to control the SUBJECT DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software, and evidence of the lack of such malicious software.
16. Evidence indicating how and when the SUBJECT DEVICES were accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user.
17. Evidence of the attachment to an item of electronic media of other storage devices or similar containers of electronic evidence.
19. Evidence of the times any item of electronic media was used.
20. Passwords, encryption keys, and other access devices that may be necessary to access any electronic media.
21. Documentation and manuals that may be necessary to access seized electronic media or to conduct a forensic examination of the media.
22. Records of or information about Internet Protocol addresses used by seized electronic media, as well as records of or information about the media's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
23. Contextual information necessary to understand the evidence described in this attachment.

Materials Relating to Trafficking in Controlled Substances
and Unlawful Possession of Firearms and Ammunition

24. Any and all photographs, videos, chats, chat logs, emails, and other text documents, describing or relating to drug trafficking and/or unlawful possession of firearms and ammunition (*i.e.*, TARGET OFFENSES).
25. Any and all address books, names, and lists of names and addresses of co-conspirators engaged in drug trafficking and/or unlawful possession of firearms and ammunition.
26. Records, relating to the source of proceeds deposited to personal and/or corporate bank accounts.
27. Records relating to deposits to personal and/or corporate bank accounts and expenditures of money and wealth, to wit: money orders, wire transfers, cashier checks and receipts, bank statements, passbooks, checkbooks, and check registers.
28. Records related to the purchase of personal assets, including but not limited to real estate, vehicles, jewelry, boats and firearms and ammunition.
29. Records related to foreign or domestic travel to include but not limited to passports, documentation of travel destinations and time periods, and any and all records of expenses related to travel.
30. Records relating to the shipment, both inbound and outbound, of controlled substances and/or firearms and ammunition. This shall include, but is not limited to, packaging, packing slips, packaging materials and packaging supplies, used in the shipment of sending and/or receiving controlled substances. This shall also include proof of past shipments such as receipts and other records and indicia of mailings.